WAAP Buying Guide

Protezione end-to-end per applicazioni e API

LumIT
A DGS COMPANY

Come identificare la migliore soluzione WAAP per il tuo business?

Oggi le aziende devono dare priorità alla digital experience di clienti e dipendenti, con la conseguente necessità di trasformare e modernizzare le loro applicazioni. Se da un lato ciò contribuisce a offrire esperienze digitali migliori, dall'altro comporta delle criticità nel mantenere un'efficace sicurezza delle applicazioni.

Mentre le aziende continuano a confrontarsi con le nuove sfide di sicurezza delle applicazioni e gli aggressori evolvono le loro strategie di attacco, in molti si rivolgono a soluzioni di web app e API protection (WAAP).

Ma come scegliere la soluzione WAAP migliore per il proprio business?

F5, azienda di servizi applicativi e sicurezza multi-cloud, e LumIT, System Integrator specializzato in soluzioni di sicurezza informatica e partner di F5, mettono a tua disposizione questa guida per aiutarti a **identificare gli elementi da prendere in considerazione per la scelta del WAAP**.

Contenuti

Cos'è il WAAP?

Le aziende che forniscono esperienze digitali sicure otterranno un vantaggio competitivo, rilasciando in sicurezza applicazioni innovative che attraggono e soddisfano i clienti. Tuttavia, il cambiamento delle dinamiche nel modo in cui le applicazioni vengono progettate e distribuite ha ampliato la superficie delle minacce e ha reso necessario un cambiamento di paradigma nel modo in cui la sicurezza viene erogata.

Gli sforzi per rimanere all'avanguardia in un mondo digital-first grazie allo sviluppo di applicazioni moderne, alle metodologie Agile e all'automazione vengono compromessi da **attaccanti evoluti che abusano di app e API**, provocando violazioni di dati, tempi di inattività e account takeover (ATO). La situazione è ulteriormente aggravata dall'attrito nella customer experience. I rigidi controlli di sicurezza scoraggiano involontariamente i clienti (e gravano sui team InfoSec con gli alert) e le conseguenti performance al di sotto delle aspettative possono portare all'abbandono delle transazioni e del marchio.

I responsabili della sicurezza e della gestione del rischio devono tutelare il business proteggendo le app e le API e operando alla stessa velocità del mercato. È necessario ridurre al minimo i test di sicurezza e le messe a punto manuali, che rallentano il ciclo di rilascio, e minimizzare il verificarsi di falsi positivi, che comportano perdite di tempo, andando contemporaneamente a incrementare le prestazioni e l'usabilità per migliorare l'esperienza del cliente.

Un numero sempre maggiore di aziende sta prendendo in considerazione soluzioni Saas distribuite in cloud per gestire la complessità della messa in sicurezza delle esperienze digitali. In particolare, **la web app e API protection, ovvero il WAAP**. Le applicazioni si stanno sempre più evolvendo verso architetture multi-cloud altamente distribuite, guidate da prestazioni, conformità e interoperabilità dell'ecosistema. Questo cambiamento di paradigma nel modo in cui le applicazioni vengono progettate e distribuite introduce nuovi rischi architetturali.

Le API sono soggette agli stessi tipi di rischi delle applicazioni web tradizionali e gli aggressori sanno che la complessità delle moderne app gioca a loro favore: i team di sicurezza non riescono a tenere il passo con un tessuto di touchpoint digitali in continua evoluzione e con un calcolo dei rischi sempre più difficile. L'osservabilità, le informazioni utili e la protezione end-to-end che utilizza il machine learning per adattarsi alle minacce emergenti sono un must per la sicurezza multi-cloud.

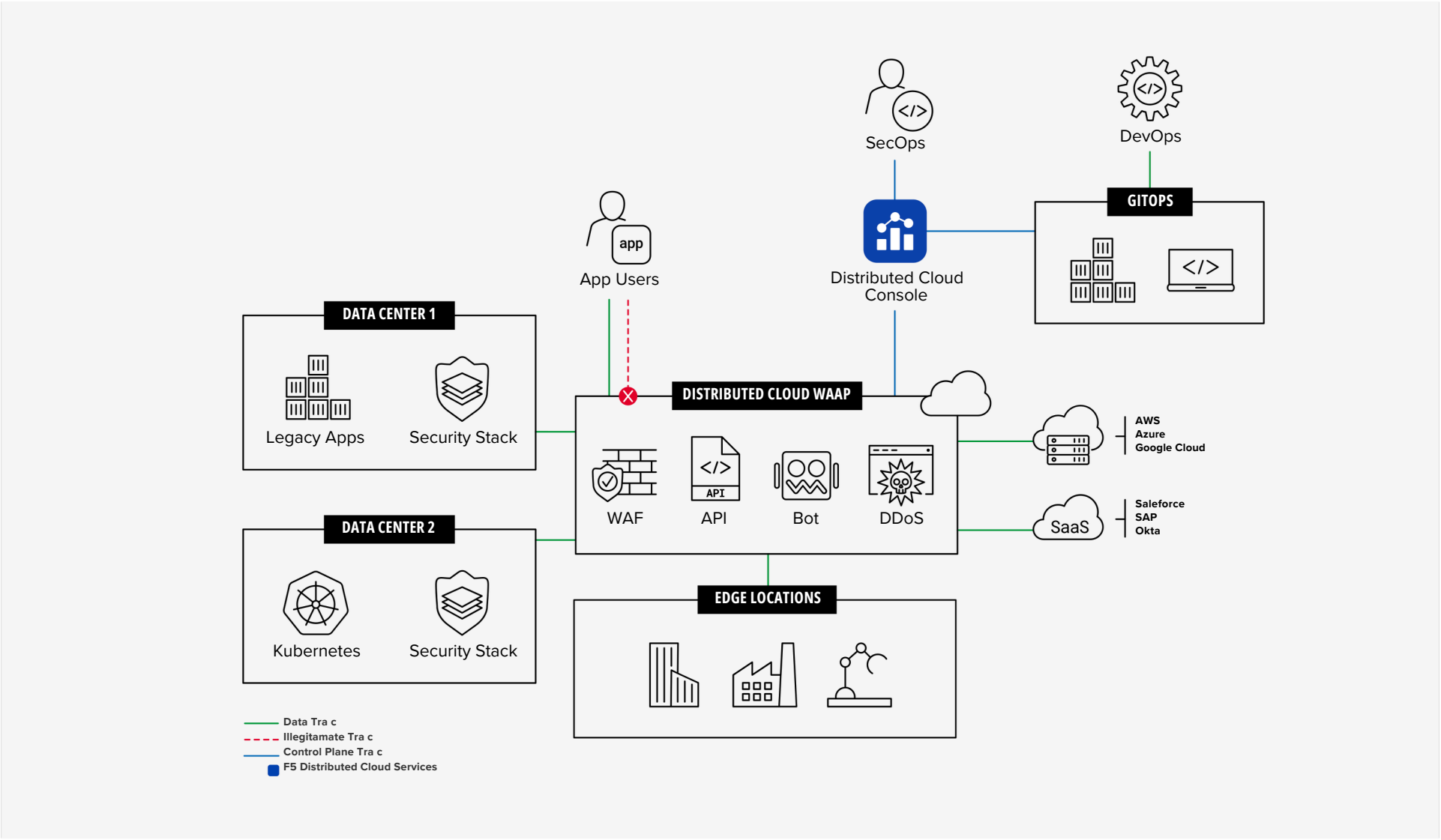


Figure 1 Web App and API Protection.

Perché le aziende hanno bisogno del WAAP?

I leader aziendali sono alle prese con cambiamenti e incertezze senza precedenti, mentre il ritmo della trasformazione digitale continua ad accelerare, costringendo ad allineare e rafforzare meglio le alleanze tra i team di sicurezza e i team dedicati allo sviluppo di applicazioni. La complessità della gestione delle applicazioni, sia legacy che moderne in ambienti ibridi e multi-cloud, ha portato a frizioni tra i team responsabili della sicurezza e delle applicazioni, alla frustrazione dei clienti e a una maggiore vulnerabilità agli attacchi.

Complessità

La sfida più grande è la complessità, causata da una proliferazione di architetture che deriva dalla costante necessità di fornire funzionalità e feature per ottenere un vantaggio competitivo. Ad esempio, la pressione per innovare rapidamente ha portato all'adozione su larga scala di integrazioni di terze parti tramite API, che possono introdurre rischi sconosciuti per l'azienda, soprattutto quando queste interdipendenze non sono di competenza dei team di sicurezza.

Applicazioni Legacy e Applicazioni Moderne

La decentralizzazione architetturale e il moderno sviluppo del software hanno portato alla creazione di una serie di risorse che devono essere protette, aumentando in modo significativo il rischio di compromissione quando le organizzazioni mantengono applicazioni legacy e nuovi cataloghi digitali. Mentre gli stack web personalizzati a tre livelli nel data center hanno ancora un posto, il cloud, i microservizi e le tecnologie dei container, come le API, hanno favorito un'esplosione dell'innovazione che i team applicativi sfruttano per migliorare le loro capacità digitali. Il ritmo della proliferazione di architetture e strumenti sta rendendo insostenibili le pratiche di sicurezza manuali.

Frizione e frustrazione

I team di sicurezza possono faticare a tenere il passo con i rapidi rilasci di funzionalità e codice che sfruttano componenti open source e di terze parti con conseguenti opportunità perse e attriti interni. Con così tanti modi di acquistare nell'economia digitale i clienti sono diventati intolleranti agli attriti dovuti a un'eccessiva autenticazione che impedisce loro di effettuare transazioni. Le aspettative dei clienti spingono inoltre a distribuire i touchpoint digitali più vicino all'edge, in quanto qualsiasi intoppo nelle prestazioni può causare l'abbandono delle transazioni e persino del brand.

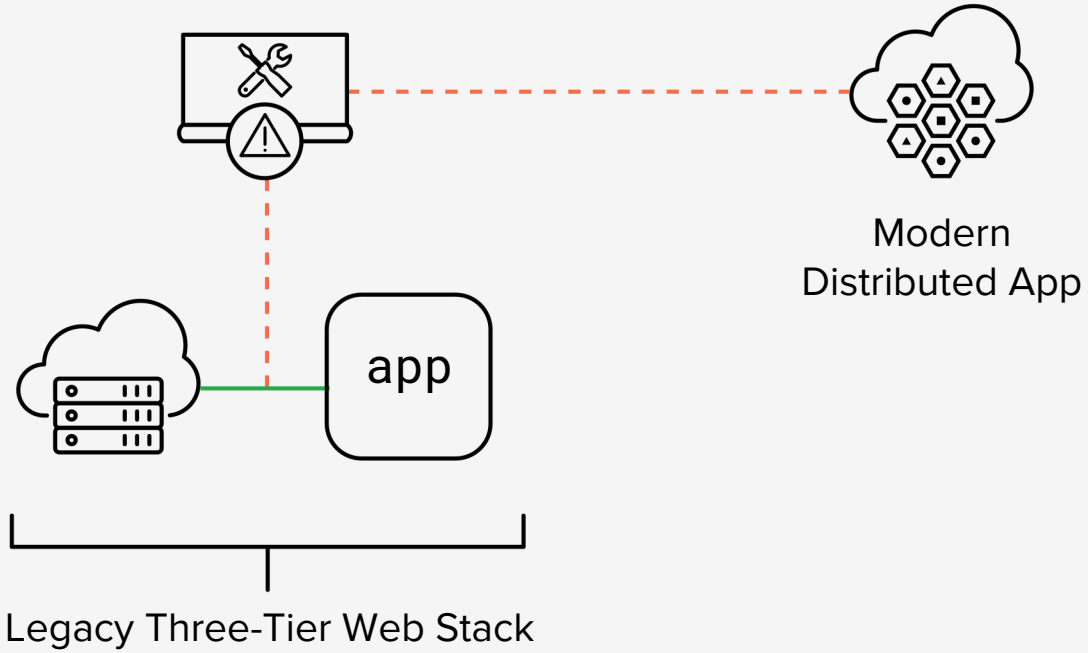
Entro il 2031 saranno in uso oltre un miliardo di API. 1*

L’economia del cybercrime

La complessità della gestione delle applicazioni moderne, legacy e decentralizzate, ha reso più attraente l'economia del cybercrime. Una cadenza costante di vulnerabilità, exploit e credenziali compromesse continua a espandere la superficie di attacco, mentre strumenti automatizzati sofisticati e infrastrutture di botnet prontamente disponibili offrono agli aggressori un ROI interessante per i loro sforzi.
I criminali e gli attori statali più sofisticati non si lasciano scoraggiare facilmente e si riorganizzano costantemente per eludere il rilevamento.

In media, **una** richiesta di autenticazione **su cinque** proviene da sistemi automatizzati dannosi, come le botnet per il credential stuffing.2*

Figure 2: Complexity driven by architecture decentralization dramatically expands the threat surface.



Cosa rende efficace un WAAP?

Esiste una chiara opportunità per le organizzazioni che sfruttano la sicurezza come vantaggio competitivo per proteggere il business e soddisfare i clienti. Integrando la sicurezza nei framework di sviluppo, distribuendo le attività di controllo in prossimità di app e API e adattandosi continuamente sia alle condizioni di sicurezza che alle prestazioni, l'azienda può concentrarsi sul profitto e sul coinvolgere i clienti con esperienze digitali efficaci. Le piattaforme in grado di astrarre le complessità dei diversi ambienti - sia che i touchpoint digitali si trovino nel data center, nel cloud privato, nel cloud pubblico o all'edge - di applicare in modo coerente i criteri e di rimediare automaticamente alle minacce rappresentano il modo migliore per i team di sicurezza di tenere il passo con la velocità del business digitale. La valutazione e la mitigazione dei rischi devono sfruttare la telemetria durevole e il machine learning altamente addestrato per mantenere la resilienza, soprattutto quando i criminali informatici adottano l'intelligenza artificiale per migliorare le loro campagne. Fondamentalmente, la visibilità e l'enforcement sono ancora considerazioni di primaria importanza.

9 organizzazioni su 10 che operano in multi-cloud segnalano la complessità degli strumenti e delle API.3*

Visibilità

Deployment

Una sicurezza efficace e facile da usare si distribuisce in modo coerente tra cloud e architetture, si integra nelle pipeline CI/CD e si aggiorna con un'intelligence continua sulle minacce.

Policy Tuning

La sicurezza che si adatta all'evoluzione delle applicazioni e delle minacce, grazie al machine learning e alla supervisione umana, riduce continuamente i rischi di compromissione e di abuso.

Enforcement

Discovery

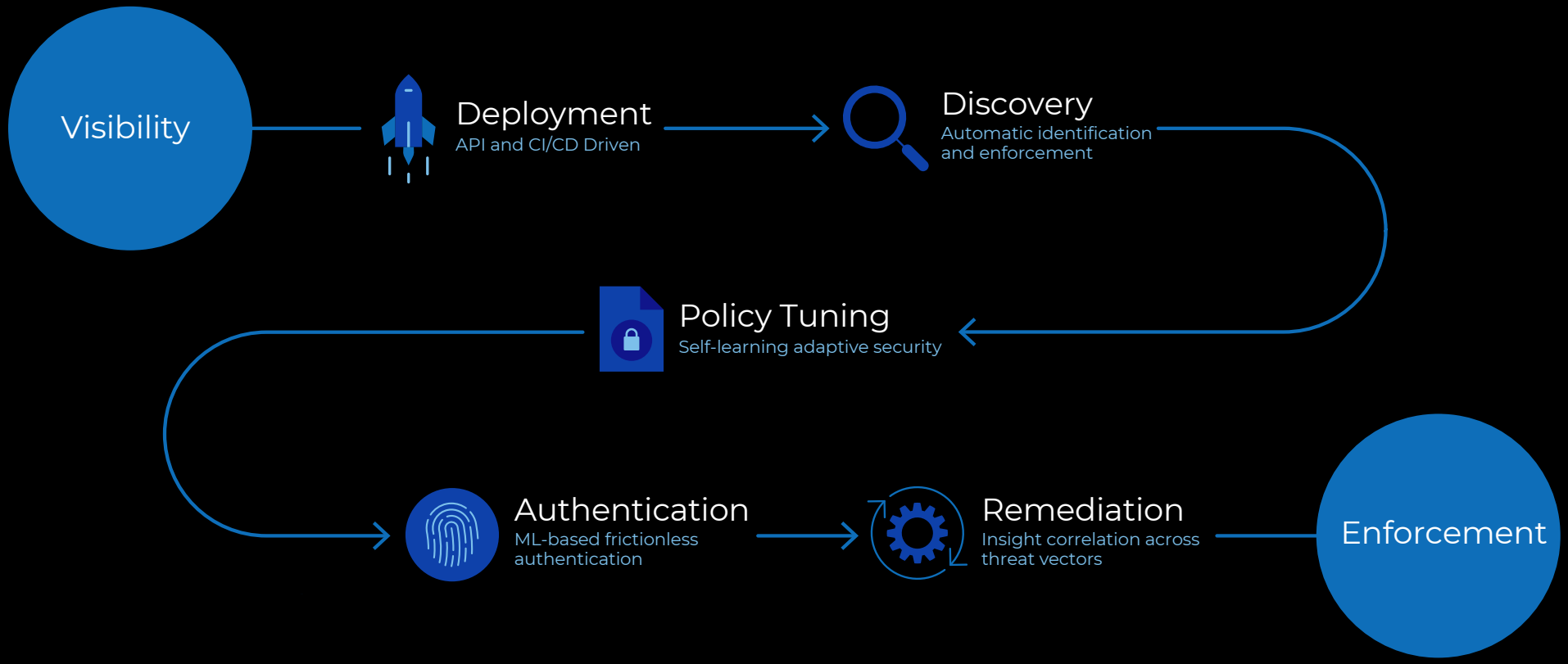
La rilevazione dinamica delle API con il riconoscimento delle anomalie, l'analisi comportamentale e il risk scoring automatizzato proteggono dai rischi involontari nell'economia digitale guidata dalle API.

Autenticazione

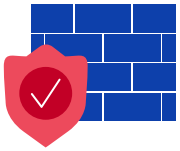
Una telemetria accurata e duratura con un'intelligenza artificiale altamente qualificata permette di ridurre drasticamente la complessità dei processi di autenticazione, evitando così di compromettere l'esperienza del cliente.

Remediation

La mitigazione e la correzione automatizzata dei falsi positivi e la correlazione degli insight tra i vari vettori delle minacce riducono al minimo gli oneri operativi e consentono all'InfoSec di concentrarsi sul rischio e sulla risposta agli incidenti.


Visibility
Deployment
API and CI/CD Driven
Discovery
Automatic identification and enforcement
Policy Tuning
Self-learning adaptive security
Authentication
ML-based frictionless authentication
Remediation
Insight correlation across threat vectors
Enforcement

Quali elementi rendono un WAAP il migliore?



Sicurezza efficace

La migliore soluzione WAAP assicura la resilienza dell'infrastruttura, con attriti e falsi positivi minimi, grazie alla mitigazione in tempo reale, all'analisi retrospettiva e alla sicurezza adattiva.

- La sicurezza robusta, la threat intelligence e il rilevamento delle anomalie proteggono in tempo reale tutte le app e le API da exploit, botnet, abusi e denial-of-service per prevenire compromissioni, violazioni di dati, ATO e tempi di inattività.
- Gli insight correlati su più vettori e la valutazione basata sul machine learning degli eventi di sicurezza, dei fallimenti dei login, dei policy trigger e dell'analisi comportamentale consentono l'autoapprendimento continuo e il rilevamento degli utenti malintenzionati.
- Le contromisure di sicurezza autonome, che reagiscono quando gli aggressori si riorganizzano, ingannano e arrestano gli attaccanti senza la necessità di ricorrere a mitigazioni che inficiano l'esperienza del cliente.

Facile da usare

La migliore soluzione WAAP offre un'implementazione self-service con una bassa complessità operativa grazie a un onboarding semplice, una protezione automatizzata e una reportistica interattiva.

- La sicurezza che sfrutta il self-learning e il self-tuning si integra nella gestione degli eventi e negli ecosistemi CI/CD per ridurre il carico dei team InfoSec, DevOps e AppDev.
- La rilevazione dinamica e le baseline delle policy consentono la mitigazione automatica, la messa a punto e la correzione dei falsi positivi durante l'intero ciclo di vita dello sviluppo/deployment e oltre.
- Una suite di dashboard di sicurezza con punteggio di rischio e drill-down contestuale massimizza la potenza della correlazione degli insight per la risposta agli incidenti e la forensics.

Piattaforma distribuita

La migliore soluzione WAAP offre visibilità universale e applicazione coerente delle policy su tutti i cloud e le architetture.

- I punti di inserimento per data center, cloud, container e CDN facilitano una visione completa dell'intero portafoglio di applicazioni.
- Le policy dichiarative astraggono dall'infrastruttura sottostante per evitare configurazioni errate.
- La sicurezza viene implementata on-demand dove necessario per garantire una protezione uniforme dall'app all'edge.

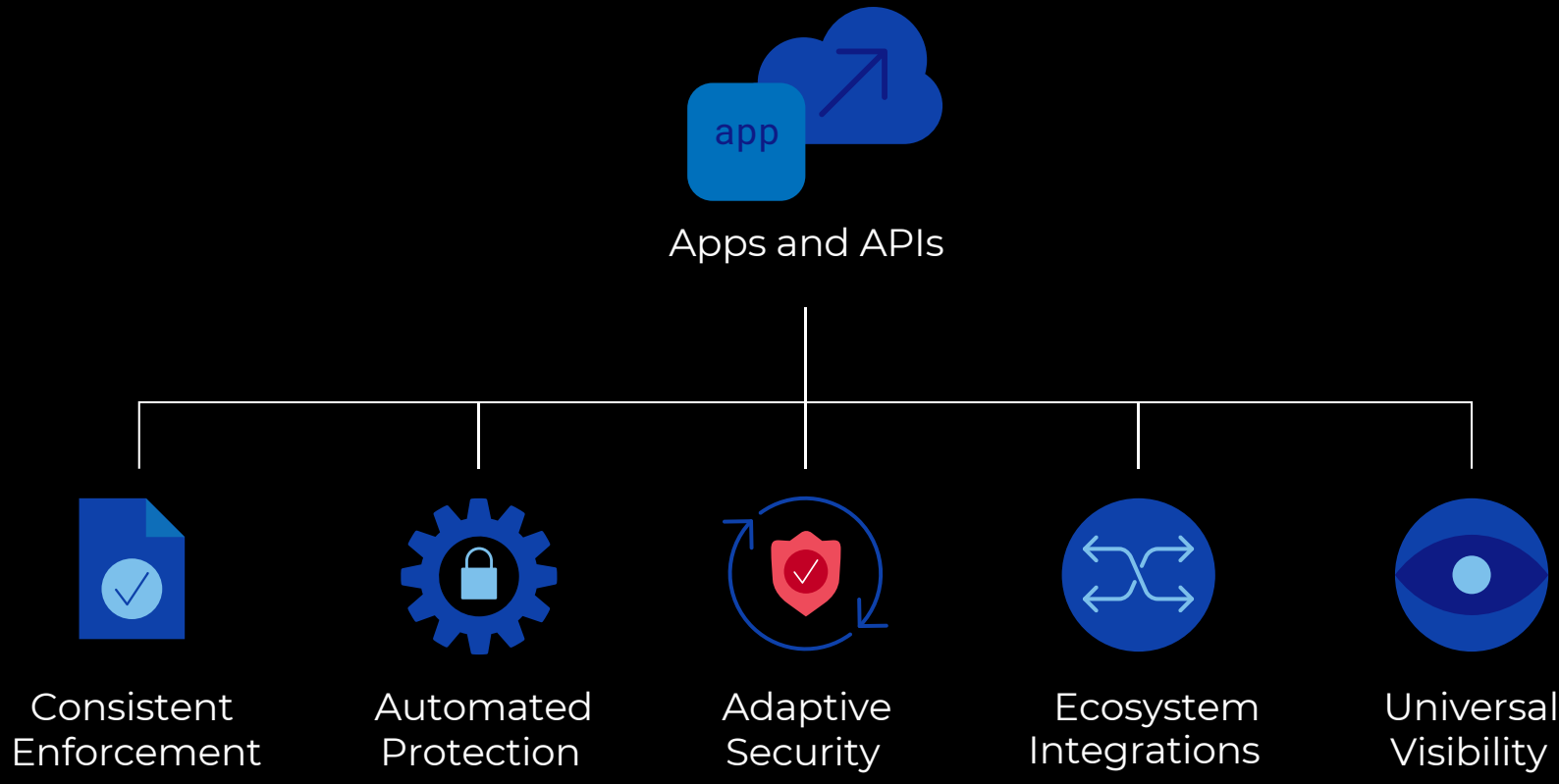
Protezione delle API

La migliore soluzione WAAP rileva in maniera dinamica e protegge in automatico tutti i touchpoint digitali.

- Piattaforma distribuita universale con analisi dei dati durature e actionable insight.
- Rilevamento e verifica continui dei potenziali endpoint rogue - shadow e zombie API.
- Supporto su protocolli diversificati (REST, GraphQL, gRPC), applicazione dello schema API e sicurezza automatizzata basata su machine learning.

Gli elementi chiave di un WAAP efficace

La migliore soluzione WAAP fornisce visibilità universale e applicazione coerente delle policy in ambienti ibridi e multi-cloud, utilizzando protezioni automatizzate e sicurezza adattiva per massimizzare l'efficacia e l'efficienza degli investimenti di sicurezza esistenti.



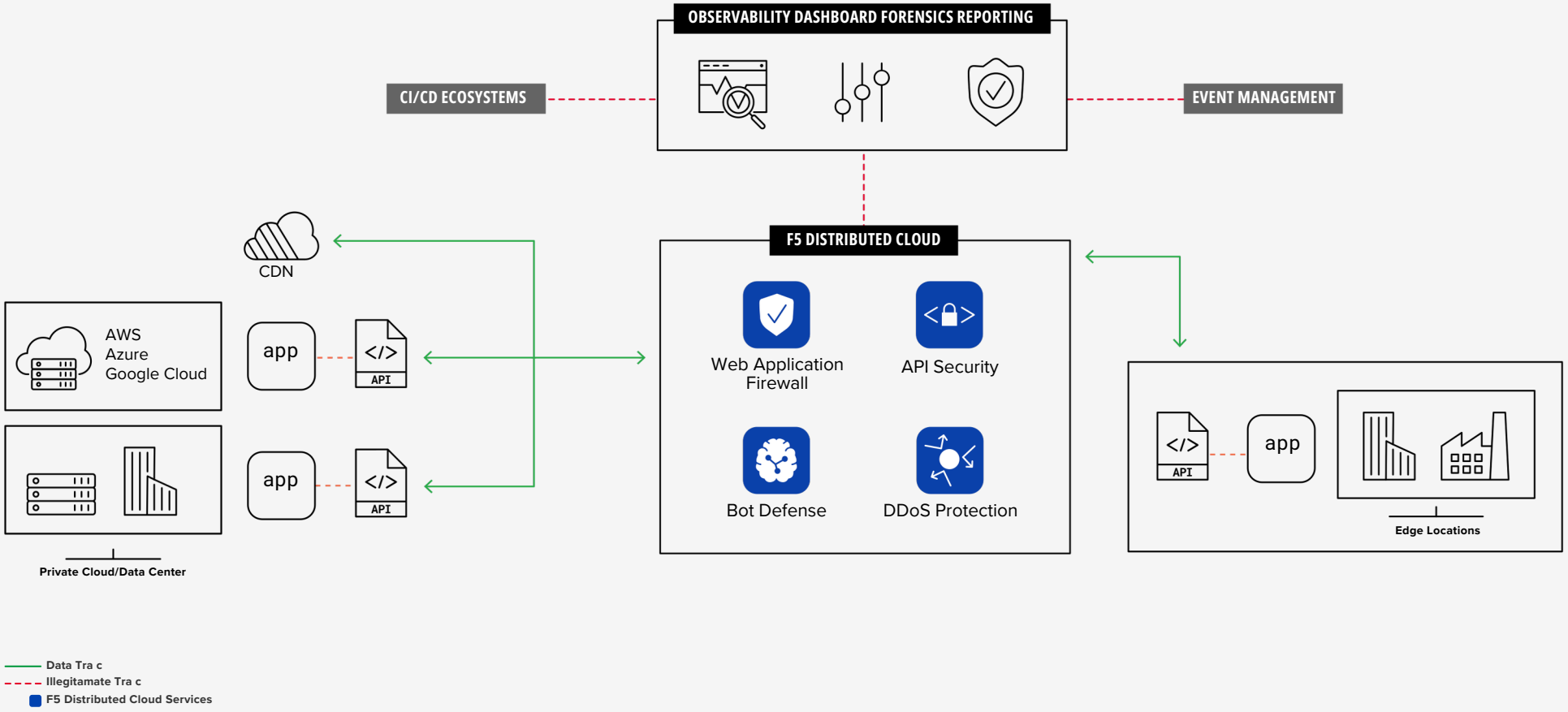


Figure 3: F5 Distributed Cloud WAAP

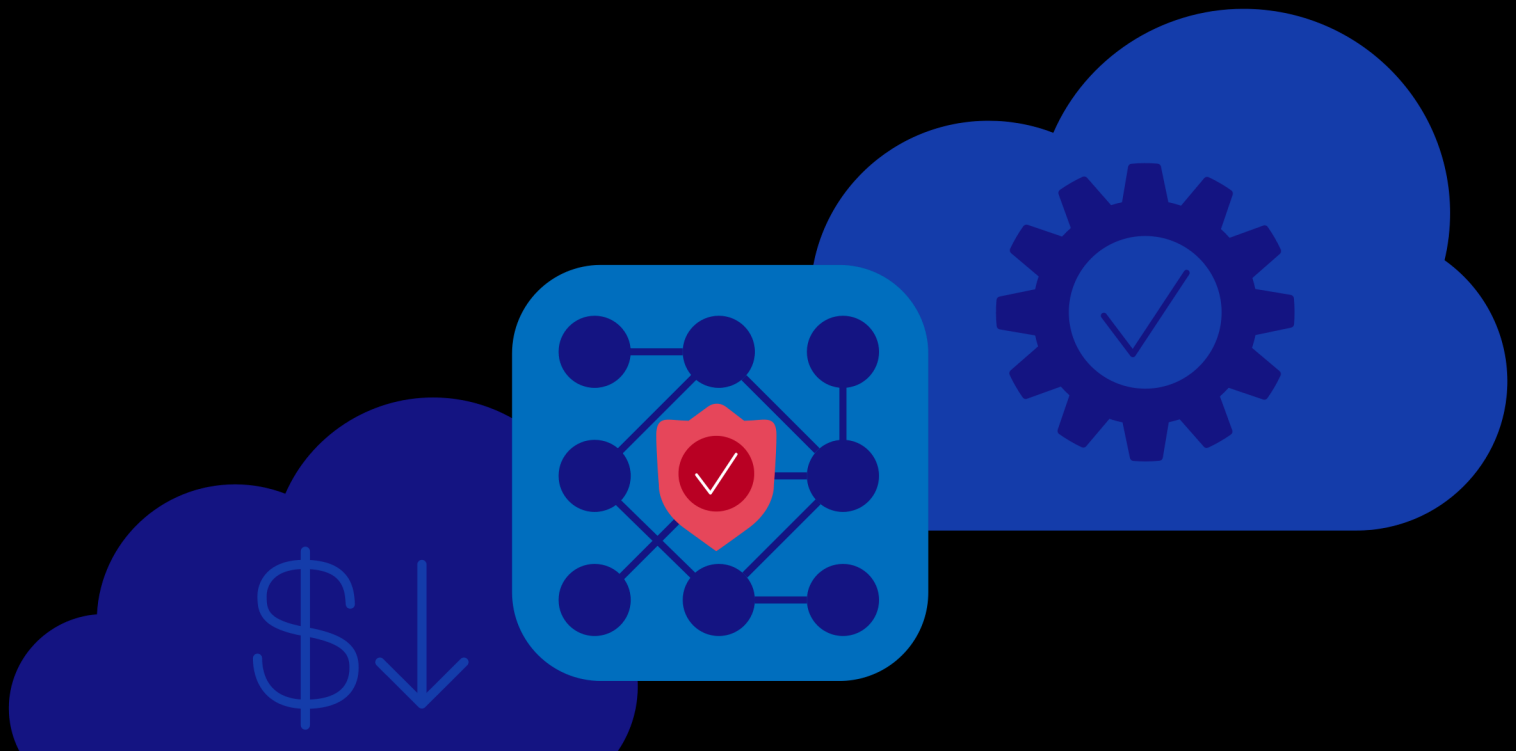
Conclusioni

Inevitabilmente, continueranno a emergere sempre nuove vulnerabilità e gli aggressori miglioreranno i loro playbook sfruttando l'intelligenza artificiale per trarre vantaggio dalle debolezze delle architetture applicative distribuite. Le complesse catene di fornitura del software, la proliferazione del software open-source e l'automazione tramite pipeline CI/CD aumentano il rischio di vulnerabilità gravi e di configurazioni errate non intenzionali. Il rilevamento e la correzione tempestivi sono fondamentali per ridurre le falle nel software, nei protocolli critici e nei controlli di accesso. Una piattaforma con sicurezza adattiva è in grado di proteggere le applicazioni e le API in tutti i cloud e le architetture, nonché di reagire in modo continuo quando le applicazioni cambiano e gli aggressori si riorganizzano, liberando l'InfoSec dalla gestione delle regole di autenticazione personalizzate e dalla correzione dei falsi positivi.
In questo modo i responsabili della sicurezza e della gestione del rischio possono difendere il business sostenendo l'innovazione digitale.

I **servizi cloud distribuiti di F5** offrono visibilità universale, applicazione coerente, protezione automatizzata, sicurezza adattiva e integrazione dell'ecosistema nell'intero portafoglio di applicazioni, proteggendo app e API e preservando al contempo l'agilità aziendale e la customer experience.

Trasforma la prospettiva della sicurezza da centro di costo a elemento di differenziazione digitale.

Bilancia in modo efficace protezione e usabilità per offrire esperienze digitali coinvolgenti, riducendo al contempo costi e complessità.



Appendice

[1] Rajesh Narayanan and Mike Wiley, “Continuous API Sprawl: Challenges and Opportunities in an API-Driven Economy,” F5 Office of the CTO Report (2021) https://www.f5.com/pdf/reports/f5-office-of-the-cto-report-continuous-api-sprawl.pdf

[2] “2023 Identity Threat Report: The Unpatchables,” F5 Labs Report (2023) https://www.f5.com/labs/articles/threat-intelligence/2023-identity-threat-report-executive-summary

[3] “State of Application Strategy Report 2021,” F5 Report (2023) https://www.f5.com/state-of-application-strategy-report

LUMIT GOLD PARTNER DI F5

TI SUPPORTIAMO NELL'IMPLEMENTAZIONE DELLE SOLUZIONI F5

LumIT è un System Integrator specializzato in Cyber Security.
Dal 2009 offriamo alle aziende un approccio innovativo e incentrato sulle reali esigenze dei clienti.
In qualità di Gold partner di F5 e delle eccellenti competenze del nostro team tecnico siamo il partner ideale per supportarti in tutto il processo di prevendita, delivery e post vendita delle soluzioni di sicurezza per applicazioni e API con tecnologia F5.

Per saperne di più contattaci su https://lumit.it/contatti/